Nytt dokument

Eksamen IN1020 høsten 2017

Tid

13. desember kl. 14.30
Faglærerne vil gå en runde fra kl 15.30.

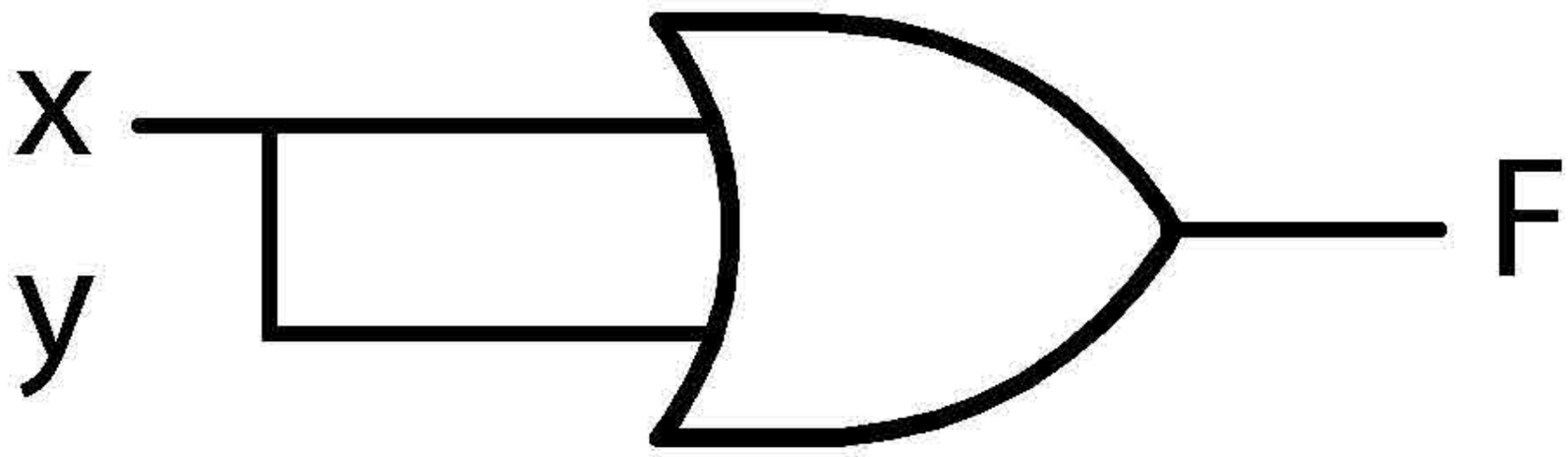
Oppgavene

Oppgavene er stort sett flervalgsoppgaver der man kan angi så mange svar man vil i hver oppgave. Noen oppgaver vil ha flere riktige svar, mens andre bare har ett. Alle vil ha minst ett korrekt svar. Man får poeng for å velge et korrekt alternativ og man mister poeng ved å velge et galt.

Tillatte hjelpemidler

Alle trykte og skrevne hjelpemidler.
En kalkulator (kun med batteri, og uten kommunikasjonsmuligheter)

2(a) Porter



Hva er utgangens funksjonsuttrykk:

Velg et eller flere alternativer

- F = x
- F = xy
- F = x + y
- F = x´

Maks poeng: 2

2(b) Teori

I emnet IN1020 har vi snakket om Flip-Flop, hva er det?
Velg et eller flere alternativer

- Kretser som man kan "flippes"
- Sandaler
- Porter som åpner
- Låsekretser

Maks poeng: 2

2(c) Teori

Hvilke av følgende utsagn er sant. (Data betyr i denne sammenheng informasjonen/bit som er lagret i minne)

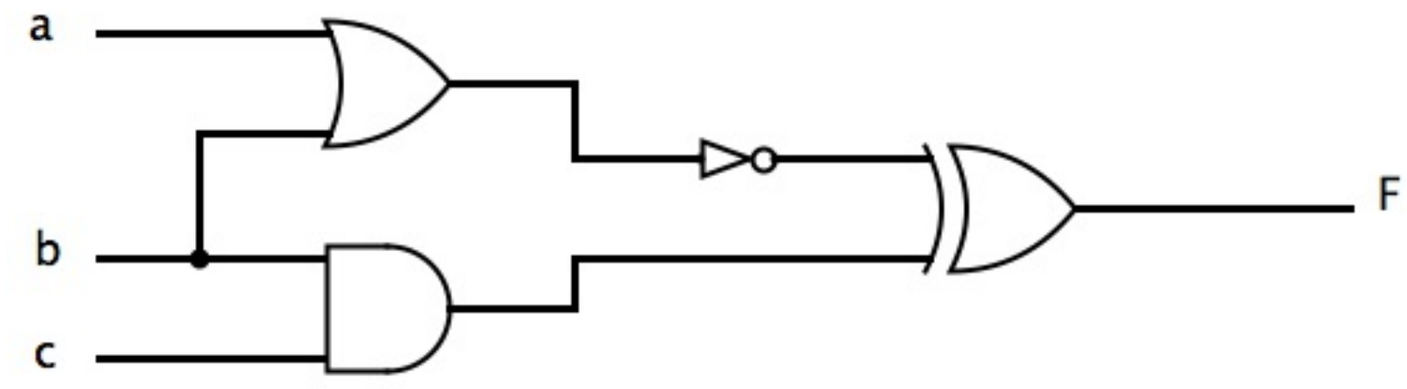
Velg et eller flere alternativer

- I minnehierarki så er det Cache som bestemmer over hva andre minneelementer (som f.eks RAM) kan lagre av data
- ALU er en sekvensiell krets som styrer hele minnehierariket.
- I minnehierarki er de minste dataene de raskeste å prosessere som gjør at de blir plassert nærmest CPUen
- I minnehierarki så er det bare harddisken som sitter med all data, de andre får bare en kopi
- I minnehierarki har de største dataene mest makt og kan overkjøre alle andre mindre dataer

---

Maks poeng: 2

2(d) Kretsanalyse



Hva er utgangsfunksjonen F gitt som:

Velg et eller flere alternativer

- F = (a´+ b´) + bc
- F = a XOR b
- F = a´b´+ b´c
- F = a
- F = ab + b´c´
- F = a´b´ + bc
- F = abc + bc
- F = (a+b)´+ (bc)

Maks poeng: 3

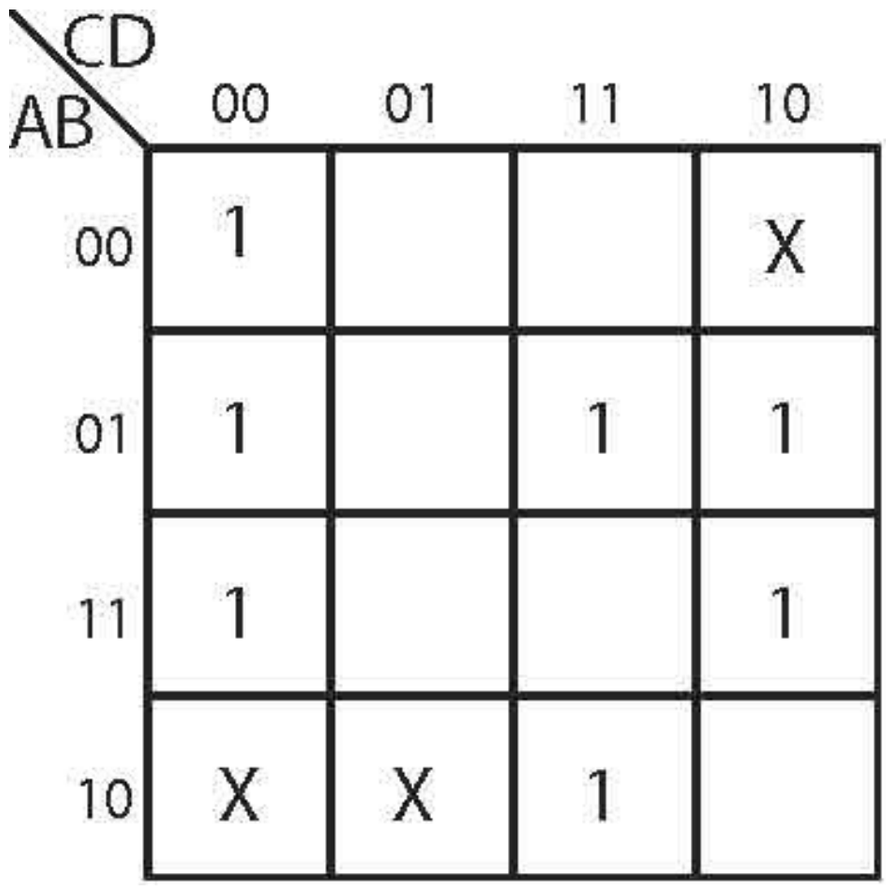
2(e) Teori

Hvilke av disse funksjonene kan en ALU i en krets gjøre:
Velg et eller flere alternativer

- Gjøre logikk operasjoner som AND, OR, NOT osv
- Øke hastigheten i kretsen ved å justere tiden det tar fra RAM til Cache
- Redusere HAZARDer ved å endre på rekkefølgen på inngangene
- Skrive data til RAM
- Addere bit
- ALU står for Aluminium og det er materialet kretsen er bygget med.
- Gjøre aritmetriske operasjoner som DIV, SUB osv

Maks poeng: 4

2(f) K-map 1



Funksjonsuttrykket for karnaughdiagrammet er:
Velg et eller flere alternativer

- F = c´d´+ ab´d + bd´+ a´bc
- F = ab´d + bcd´+ a´c´d´+ b´d´
- F = a´c´d´ + abd´+ a´bc + ab´cd
- F = bd´+ c´d´+ bc + ab´

Maks poeng: 4

2(g) Forenkling av uttrykk

Vis forenklingsprosedyren for F = $F(a,b,c) = \sum(0,2,4,6)$

Flytt alle mulige forenklingssteg i den grå firekanten.

F = a´b´c´+ a´bc´+ ab´c´ + abc´

F = c

F = abc + ab´c + a´bc + a´b´c

F = c´(a XOR b) + c´(a XNOR b)

F = ac´

F = a´c´(b´+b) + ac´(b+b´)

F = ab

F = b

F = c´(a´+a)

F = (a´b´c) + (ab´c) + (ab´c´) + (a´b´c)

F = b´c´

F = b´c´(a + a´) + ac(b + b´)

F = c´

F = (a´c´+ ac´)(b+b´)

F = (a+b+c)(a+b´+c)(a´+b+c)(a´+b´+c)

Maks poeng: 8

3(a) Binære tall 1

Verdien **27_{10}** (dvs 27 i 10-tallsystemet) kan også representeres i andre tallsystemer. Hvilke av disse verdiene er lik 27_{10}?

Velg ett eller flere alternativer:

- 102_5
- 123_4
- 1000_3
- 11001_2

Maks poeng: 3

3(b) Binære tall 2

Verdien $\mathbf{92_{10}}$ (dvs 92 i 10-tallsystemet) kan også representeres i andre tallsystemer. Hvilke verdier er lik 92_{10}?

Velg ett eller flere alternativer:

- 10102_3
- 134_8
- 108_9
- $7A_{12}$

Maks poeng: 3

3(c) Bit og byte

En byte inneholder disse bit-ene:

0	1	1	1	0	0	0	1

Hvilke verdier kan representeres av disse bit-ene?
Velg ett eller flere alternativer

- 97
- 113
- -143
- 65

Maks poeng: 3

3(d) Assembler 1

```
        .globl  f1
f1:
        movq    %RDI,%RAX
        addq    %RSI,%RAX
        subq    %RDX,%RAX
        ret
```

```
  long res = f1(1, 3, 5);
```

Hva er resultatet av kallet på funksjonen **f1**?
Velg ett eller flere alternativer (men kun ett er korrekt):

- 3
- 5
- 1
- -1

Maks poeng: 4

3(e) Assembler 2

```
        .globl  f2
f2:
        movq    $100,%RAX
        movq    v,%R10
        cqo
        idivq   %R10
        ret

        .data
v:      .quad   7
```

```
long res = f2();
```

Hva er resultatet av kallet på funksjonen **f2**?
Velg ett eller flere alternativer (men kun ett er korrekt):

- 100
- 10
- 14
- 7

Maks poeng: 4

3(f) Assembler 3

```
        .globl  f3
f3:
        movq    %RDI,%RAX
        andq    $1,%RAX
        ret
```

```
long res = f3(11);
```

Hva er resultatet av å kalle på funksjonen **f3**?

Velg ett eller flere alternativer (men kun ett er korrekt):

- 11
- 1
- 0
- 12

Maks poeng: 4

3(g) Assembler 4

```
        .globl  f4
f4:
        movq    $1,%RAX
        subq    %RSI,%RDI
        jz      f4x
        movq    $0,%RAX
f4x:
        ret
```

```
long res = f4(2, 5);
```

Hva er resultatet av å kalle på funksjonen **f4**?

Velg ett eller flere alternativer (men kun ett er korrekt):

- 0
- 1
- 5
- 2

Maks poeng: 4

4(a) Lagdeling

Hvorfor har vi lagdeling i Internettarkitekturen?
Velg et eller flere alternativer

- For at man skal kunne bytte ut komponenter som tilbyr spesifikke tjenester, uten å måtte bytte hele systemet.
- For å spare energi.
- Fordi det tok for lang tid å standardisere alle protokollene.
- Slik at ikke alle komponentene i Internettarkitekturen trenger å ha støtte for funksjonaliteten til alle lagene.

Maks poeng: 3

4(b) TCP/IP-modellen

Hvilke lag inngår i TCP/IP-modellen?
Velg et eller flere alternativer

- Det fysiske laget, Linklaget, Nettverkslaget, Sesjonslaget og Presentasjonslaget.
- Linklaget, Nettverkslaget, Transportlaget og Applikasjonslaget.
- TCP-laget og IP-laget.
- Det fysiske laget, Linklaget, Nettverkslaget, Transportlaget, Sesjonslaget, Presentasjonslaget og Applikasjonslaget.

Maks poeng: 1

4(c) Peer-to-peer

Hvilke utsagn er sanne?
En peer-to-peer aksessmodell...
Velg et eller flere alternativer

- brukes kun til ulovlige tjenester.
- kan bidra til å unngå at et selskap eller en statsmakt har kontroll over tjenesten.
- har et distribuert eierskap.
- har én sentral tjener som mottar forespørsler fra mange klienter.
- har likeverdige vertsmaskiner som samarbeider om å levere en tjeneste.

Maks poeng: 4

4(d) Subnett

Et subnett har nettverksmasken 11111111.11111111.11100000.00000000
Hvor mange gyldige IP-adresser kan tildeles verter i subnettet?
Velg et eller flere alternativer

- 254
- 8190
- 65535
- 8191
- 255
- 65534

Maks poeng: 2

4(e) Overføring

Du ønsker å laste ned en fil på 50 megabyte, og den maksimale nedlastingshastigheten på din Internettforbindelse er 20 megabit per sekund. Hva er den teoretisk korteste overføringstiden?

Velg et eller flere alternativer

- 10 sekunder
- 20 sekunder
- 50 sekunder
- 2,5 sekunder

Maks poeng: 2

4(f) UDP

Hvilke av disse tjenestene tilbys av UDP?
Velg et eller flere alternativer

- Ingen av disse
- Forbindelsesorientering
- Flytkontroll
- Sjekksum
- Bytes blir levert i samme rekkefølge som de blir sendt
- Metningskontroll
- Multiplexing over IP-adresser (porter)

Maks poeng: 3

4(g) Switch

Hva er en "switch" i datakommunikasjon?
Velg et eller flere alternativer

- En enhet som videresender pakker i linklaget.
- En tjeneste som tildeler IP-adresser til maskiner i et lokalt nettverk.
- En enhet som videresender datapakker innenfor et lokalt nettverk (LAN).
- En bryter som skrur av datamaskinen.
- En enhet som videresender IP-pakker til andre subnett i Internett.

Maks poeng: 3

4(h) Broadcast

Hvorfor bør ikke et kringkastingsdomene (broadcast domain) / subnett være for stort?
Velg et eller flere alternativer

- Støyen fra broadcast-trafikk (f.eks DHCP og ARP) kan bli for stor og gå ut over ytelsen i nettverket.
- Det tar for lang tid å route trafikken via alle maskinene.
- Det går helt fint så lenge topologien er et stjernenett.
- Oppslag i ARP-tabellene tar for lang tid.

Maks poeng: 1

4(i) HTTP - Del 1

Hvilket av disse utsagnene er korrekt for en persistent forbindelse i HTTP?
Velg et eller flere alternativer

- HTTP-forespørsler kan ikke multiplekses over denne forbindelsen.
- Den samme TCP-forbindelsen blir gjenbrukt til flere runder med nye HTTP-forespørsler.
- TCP-forbindelsen fortsetter å forsøke å koble seg opp, selv om den blir avsluttet eller brutt.
- Nyttelasten sendes mange ganger uavhengig av nettverksforhold for å være sikker på at de kommer frem.

Maks poeng: 1

4(j) NAT

Hvilken tjeneste tilbyr Network Address Translation (NAT)?
Velg et eller flere alternativer

- Den gjør det lettere for maskiner på Internett å koble seg på maskiner i det lokale nettverket.
- Den oversetter mellom MAC-adresser og IP-adresser.
- Den gjør det mulig for mange enheter på et lokalt nettverk å dele én ekstern/offentlig IP-adresse.
- Den kringkaster hvilket portnummer som benyttes av en bestemt tjeneste.

Maks poeng: 1

4(k) HTTP - Del 2

Hvilke utsagn er sanne?

Multipleksing av HTTP-forespørsler...

Velg et eller flere alternativer

- ...betyr at klienten sender flere forespørsler, og tjeneren kan sende svar på alle i en rekkefølge bestemt av tjeneren selv.
- ...innebærer at for hver forespørsel som sendes, må man vente på svar før neste forespørsel sendes.
- ...betyr at tjeneren kan "gjette" hvilke forespørsler som kommer og sende svar før den har mottatt forespørselen.
- ...betyr at klienten sender flere forespørsler, og tjeneren kan sende svar på alle i samme rekkefølge som forespørslene kom inn.

Maks poeng: 2

4(I) DNS - Del 1

En rottjener i DNS-hierarkiet tar vare på følgende
Velg et eller flere alternativer

- En liste over DNS-tjenerne til Top Level Domains (TLDs).
- En liste over IP-adresser og hvilken MAC-adresse som hører til den.
- En oversikt over alle IP-adresser i en organisasjon (f.eks. uio.no).
- En liste over ledige offentlige IP-adresser på Internett.

Maks poeng: 1

4(m) DNS - Del 2

Hva er DNS-prefetching?
Velg et eller flere alternativer

- En hjemmerouter lagrer DNS-oppslag slik at brukeren ikke behøver å kontakte en rottjener.
- En tjeneste mellomlagrer MAC-adressen til webtjenere for raskt oppslag.
- En tjener mellomlagrer hjemmesider, slik at forespørselen ikke trenger å gå helt til kilden.
- En nettleser slår opp IP-adressen på alle domenenavn (URLer) den finner i et webdokument for å spare tid i tilfelle brukeren trykker på linken.

Maks poeng: 1

5(a) Sikkerhetsmål

Sikkerhetsmål er et sentralt begrep innen informasjonssikkerhet. Hvilke av følgende defineres som sikkerhetsmål:

Velg et eller flere alternativer

- Uavviselighet
- Tilgangskontroll
- Biometri
- Autorisering
- Identifikasjon
- Datakryptering
- Systemautentisering
- Tilgjengelighet

Maks poeng: 2

5(b) Sikkerhetstiltak 1

A) Hvilke sikkerhetstiltak kan bidra til å oppnå sikkerhetsmålet konfidensialitet?
Velg et eller flere alternativer

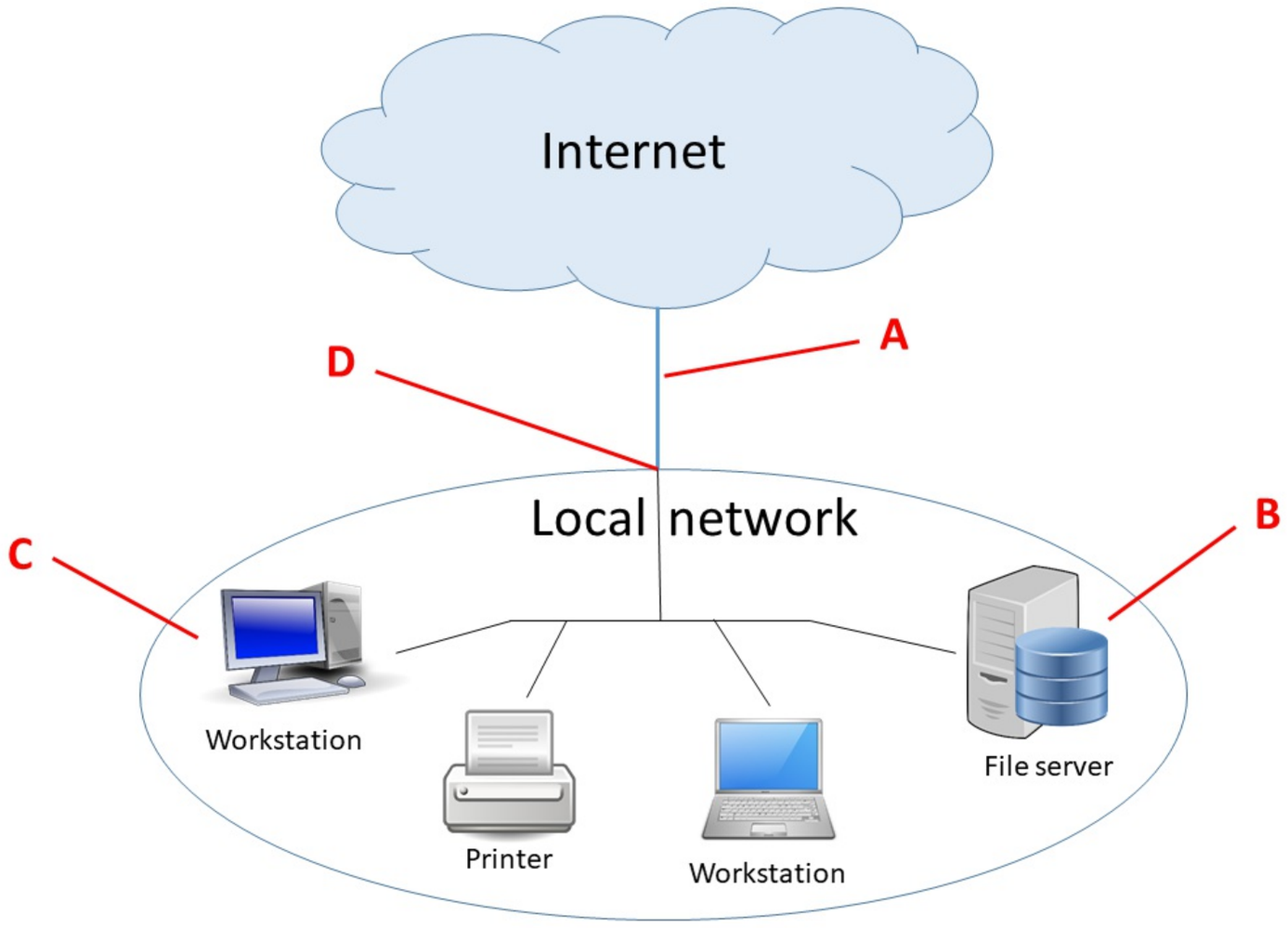
- Identifisere og autentisere brukere
- Brukeropplæring
- Redundante tjenester
- Kryptering
- Tilgangskontroll
- Logging av hendelser

B) Hvilke sikkerhetstiltak kan bidra til å oppnå sikkerhetsmålet sporbarhet?
Velg ett eller flere alternativer

- Kryptering
- Tilgangskontroll
- Brukeropplæring
- Redundante tjenester
- Logging av hendelser
- Identifisere og autentisere brukere

Maks poeng: 3

5(c) Sikkerhetstiltak 2



Figuren over illustrerer et lokalt nettverk knyttet til internett.

Hvilke sikkerhetstiltak passer inn på hvilke sted i figuren? Knytt sammen bokstav med tiltaket du mener passer.

	C	A	B	D
Brukeropplæring	○	○	○	○
Sikkerhetskopiering	○	○	○	○
Brannmur	○	○	○	○
Innbruddsdeteksjon	○	○	○	○
Kryptert trafikk	○	○	○	○

Maks poeng: 3

5(d) Tilgangskontroll

Hva er de gunnleggende elementene i et system for tilgangskontroll:
Velg et eller flere alternativer

- Autentisering, privilegier og brukeridentitet.
- Passord, tilgang og kryptografi.
- Identifikasjon, autentisering og autorisering.
- Delte nøkler, autorisering og brukeridentitet.

Maks poeng: 2

5(e) Autorisering

Autorisering er et begrep innen informasjonssikkerhet. Hva kjennetegner autorisering:
Velg et eller flere alternativer

- Passord benyttes som autentikator for autorisering av entiteter, roller og prosesser.
- Å autorisere betyr å spesifisere tilgang og brukerrettigheter for entiteter, roller og prosesser.
- At en identitet er autentisert i et system betyr at identiteten også er autorisert i det samme systemet.
- Autorisering følger et forhåndsdefinert regelsett (policy).

Maks poeng: 3

5(f) Skadevare

Skadevare er en samlebetegnelse på programvare som med hensikt gjør skade på et datasystem.

Knytt sammen riktig funksjon og benevnelse på skadevaren:

	Tastelogger	Orm	Logisk bombe	Bakdør	Virus
Gir tilgang til et system via ukjent inngang	○	○	○	○	○
Sprer seg når det kjøres	○	○	○	○	○
Overvåker all tastatur-input fra brukeren	○	○	○	○	○
Kjøres når spesielle forhold inntreffer eller oppfylles	○	○	○	○	○
Sprer seg på egenhånd til andre datasystemer	○	○	○	○	○

Maks poeng: 3

5(g) Personvern

I "Lov om behandling av personopplysninger (personopplysningsloven)" skilles det mellom ordinære personopplysninger og sensitive personopplysninger.

Merk: Alle sensitive personopplysninger er i utgangspunktet også personopplysninger, men her er oppgaven å kategorisere de sensitive personopplysningene som nettopp sensitive.

Plasser følgende personopplysning i rett kategori:

	Ordinær personopplysning	Sensitiv personopplysning
Hodeform	○	○
Irismønster	○	○
Dømt for straffbar handling	○	○
IP-adresse	○	○
Medlemskap i idrettslag	○	○
E-postadresse	○	○
Medlemskap i fagforening	○	○
Mistenkt for straffbar handling	○	○

Maks poeng: 2

5(h) Kryptografi og nøkkelutveksling

Kryptografi benyttes for å beskytte informasjon mot innsyn og modifikasjon. For å kryptere og dekryptere informasjon benyttes kryptografiske nøkler. Ved assymetrisk kryptering benytter man seg av et nøkkelpar som består av en privat og en offentlig nøkkel.

Hvilke sikkerhetsmål bør oppnås for å sikre trygg oppbevaring av en offentlig assymetrisk nøkkel?
Velg et eller flere alternativer

- Den offentlige nøkkelen må oppbevares på en måte som sikrer nøkkelens integritet og ektehet.
- Den offentlige nøkkelen er allmenn tilgjengelig, og trenger derfor ingen spesiell beskyttelse.
- Det er viktig å vite hvem som benytter en offentlige nøkkel, og brukere og systemer må derfor autentisere seg før bruk for å kunne sikre sporbarhet.
- Den offentlige nøkkelen må oppbavares på en måte som sikrer konfidensialitet samt nøkkelens integritet og ektehet.

Maks poeng: 2.5

5(i) Trusselmodellering 1

Et helseforetak behandler og lagrer en rekke opplysninger om pasienter, til dels av sensitiv karakter. Systemet er lukket, og ikke tilkoblet andre nettverk enn det interne nettverket for akkurat dette systemet.

Hvilke av følgende utsagn vil du betegne som sanne på bakgrunn av disse opplysningene:

Velg et eller flere alternativer

- Helseforetaket bør ha en nøye utarbeidet policy for hvilke ansatte som har tilgang til å lese, endre og slette opplysninger om hvilke pasientene.
- Siden systemet er lukket er det ingen risiko for angrep utenfra, og det er derfor ikke nødvendig å prioritere sikring av informasjon høyt.
- Fysisk sikring av systemets endenoder (f.eks. de ansattes arbeidsplassmaskiner) er spesielt viktig.
- Å sikre sporbarhet er ikke viktig hvis man har gode mekanismer for autentisering på plass, for eksempel tofaktor-autentisering.

Maks poeng: 3

5(j) Trusselmodellering 2

Løsepengevirus er en type skadevare som blant annet infiserte et stort antall datamaskiner verden rundt våren 2017.

Kryss av for tiltak som kan iverksettes for å minimere risikoen for å bli rammet av et løsepengevirus:

- Filkryptering
- Streng tilgangskontroll
- Antivirus
- Sikkerhetsoppdateringer
- Sikkerhetskopier

Maks poeng: 1.5